REMARKS

Reconsideration of the above-mentioned application in view of the amendments above and the following remarks is respectfully requested.

Claims 1 – 30 are pending in the current application. Claims 1 and 16 have been amended.

Claim Objections

Claim 1 was objected to as being missing a period at the end. Applicant has hereby amended Claim 1 to delete the semicolon and to add a period.

Claims Rejection under 35 USC §102

Claims 1-30 were rejected under 35 U.S.C. 102 as being anticipated by Schwartz (US Patent application 2001/0044787). Applicant respectfully traverses the Examiner's rejections.

The present invention provides a system and method for allowing a user to perform a securely and anonymously purchase of merchandise over a non-secure public network such as the Internet. The system provides high security by avoiding transmission of sensitive information over the network and overcomes psychological inhibitions by allowing the user to use his/her credit card in a manner which is very similar to the manner credit cards are conventionally used. This is achieved by providing the user with a novel <u>hardware component</u> referred to as a safe payment unit or pay-safe unit (PSU, designated as item 150 in the drawings, in particular see Fig. 3 and the paragraph beginning at line 12 on page 11). The safe payment unit is a separate portable hardware unit connectable to the user computer. The unit includes a <u>card reader</u> (156), CPU, memory, an authentication protocol and means to connect via

8

a telephone line to a trusted agent. In accordance with the method of the present invention, after initiating a transaction over a public network and if the user chooses paying via the safe payment route, the transaction data is downloaded into the PSA. The user is then triggered to insert his/her credit card to the card reader of the PSU and following the card authentication by the PSU, an off-the-net secure telephone channel is opened between the PSU and the trusted agent for transferring sensitive data and for completion of the transaction. The transactions performed in accordance with the present invention are therefore of the so called "a card present transaction" type since they require the actual insertion of the card into the PSU card reader. Furthermore, in accordance with the invention, the PSU may be user-specific, i.e., dedicated to a specific card or a number of specific cards, such that a transaction is processes only if a match is found between the card and the PSU (see the second full paragraph of page 15, beginning at line 17). This further enhances the security of the transactions. Furthermore, in accordance with the invention, the trusted agent is the credit card issuer or a mediator agent mediating between credit card users and credit cards issuer companies. Thus, a user (either a customer or a vendor) does not need to establish a relationship with a new financial agent or to sign into a new agreement as the agreement he/she has with regard to their credit card may apply as well to the transactions over the Internet. This saves the user the inconvenience of new registrations, new agreements and the need to remember new procedures and codes.

U.S. Patent Application Publication 2001/0044787 (hereinafter "Schwartz"), cited by the Examiner, teaches a system aimed at a similar purpose as that of the present invention, namely anonymous and secured electronic transactions over a public network. However the system and method taught by Schwartz are very different form the present invention. The solution taught by Schwartz is the provision of a computer implemented trusted third party referred to as "secure private agent" (SPA) which acts as an agent for the customer. The secure private agent is a software application that can be implemented either as a client application in the customer's computer or can reside elsewhere in the data network

as a server application in a clientless mode. In the latter case, the client logs-in to the SPA site and then can surf from it to preferred e-commerce sites. The secure private agent, whether in a client or clientless mode, automatically monitors communication across the data network and intercepts communication between the consumer and an electronic commerce site. Thus, while the SPA is active, all information between the user and the e-commerce site is channeled through the SPA server (see for example paragraph 104 and Fig. 2 and 8). This is in contrast to the present invention where information flows directly between customer and merchant (channel 50 in Fig. 1) while an additional telephone channel (channel 60 in Fig. 1) is opened between the customer and the credit card company via the PSU. Furthermore, in accordance Schwartz, a customer has to establish a new account with the SPA which is separate from the account he/she has with the credit card company (see for example paragraph 97 and the financial rules described in paragraphs 98-102). In accordance with present invention, a user does not have to enter any passwords or codes to his/her computer in order to use the PSU. Codes, if any, are entered only to the PSU and are not passed to the computer or via the Internet (see paragraph 70). The authentication is performed locally by the PSU and via telephone line with the Credit Card Issuer. In contrast, in accordance with Schwarz, the authentication procedure is performed over the Internet in both clientless (see paragraph 134) and client mode; (See last lines in paragraphs 145 and paragraph 146). Thus, according to Schwartz, a user has to provide authentication information over a public network. This authentication information, which actually identifies the user and his/her account with the PSA, may be captured by an unauthorized party, exposing the system to possible fraud. Furthermore, a computer left unattended while the SPA mode is active allows misuse by unauthorized passerby. In contrast, in accordance with the present invention, no transaction is authorized without the actual presence of the credit card. Moreover, the portable PSU may be disconnected when not in use to be stored at a place remote from the computer.

10

The Examiner rejected Claim 1 pointing to Fig. 1 −3 and associated text in Schwartz. Applicant respectfully submits that Fig. 1-3 do not disclose the elements disclosed in claim 1. In particular, Schwartz does not teach any hardware component equivalent to the safe payment unit (150) of the present invention and/or to a card reader (156). The secure private agent taught by Schwartz comprises only software applications on the customer side. Thus, the transactions performed by Schwartz are of "non-card present" nature in contrast to the more secure "card present" transactions of the present invention. Furthermore, the communication channels are configured differently in the present invention and in Schwartz's system. The present invention provides an additional secure telephone channel (60) between the customer and the trusted agent in addition to the direct communication channel (50) between the customer and vendor over the public network. In accordance with Schwartz, the role of the SPA is to intercept direct communication between customer and vendor (channel 26) and to redirect the communication via the back end gateway through channels 24 and 28.

Regarding claims 5, 7 and 12-15, these claims relate either to features of the system associated with the safe payment unit or to additional features of the safe payment unit itself. Schwartz, not disclosing a safe payment unit, naturally do not disclose any features relating to such a unit.

Regarding method claims 16 - 30, Examiner rejected the claims on the same ground on which system claims 1-15 are rejected. Applicant respectfully submits that the above remarks in connection with the apparatus claims traverse the Examiner's rejection with respect to the method claims now pending in the application. In particular, Schwartz does not disclose the step of inserting a data card to a safe payment unit. Unlike the present invention, Schwartz does not disclose a method for performing transaction of the "card present" type. Furthermore, Schwartz teaches a method which involves automatic interception of communication between customer and e-commerce site (see step 84 in Fig. 4 and step 134 in Fig. 7) and the assignment

of virtual credit card numbers (see step 112 in Fig. 5 and step 150 in Fig. 7). These two steps are essential features of the Schwarz method. However, the present invention which provides a different solution to overcome security problems does not disclose nor claim interception of commercial transactions, or the use of virtual credit card numbers. Accordingly, applicant respectfully submits that the method taught by the present invention and the method taught by Schwarz are completely different. In order to better define the method, claim 16 was amended to better define the safe payment unit.
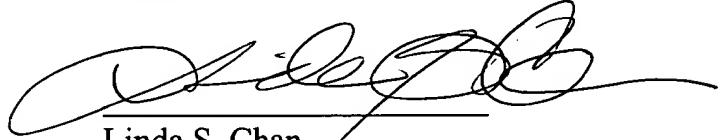
Conclusion

In view of the above remarks it is respectfully submitted that independent claims 1 and 16 are allowable rendering all dependent claims allowable as well. The issuance of a Notice of Allowance of the pending claims is respectfully solicited.

It is believed that no fee is due as a result of this amendment. However, if any fee is due with this paper, the Commissioner is hereby authorized to charge such fee to Deposit Account No. 50-1290.

12

11186606.01

Please direct any inquiries regarding this application to the applicant's undersigned attorney, who may be reached directly by telephone at (212)940-8712.

Respectfully submitted,

Linda S. Chan
Reg. No. 42,400

Attorney Docket No.: **SORO 18.955 (101121-00001)**

Customer Number: **026304**
Phone: (212)940-8800
Fax: (212)940-8776

13